Eigen schuld, dikke bult? Aansprakelijkheid bij fraude met internetbankieren

van der Meulen, N.S.

published in
Informatiebeveiliging
2012

document version
Publisher's PDF, also known as Version of record

EIGEN SCHULD, DIKKE BULT?

AANSPRAKELIJKHEID BIJ FRAUDE MET INTERNETBANKIEREN

Dr. Nicole S. van der Meulen is werkzaam als universitair docent Internet Governance bij de Faculteit Rechtsgeleerdheid van de Vrije Universiteit Amsterdam. Zij promoveerde in 2010 aan de Universiteit van Tilburg met een vergelijkend proefschrift naar identiteitsfraude in Nederland en de Verenigde Staten. Zij is te bereiken via n.s.vander.meulen@vu.nl.

Meerdere jaren geleden, in 2008, mocht ik een gesproken column voordragen tijdens een landelijke praktijk dag voor gemeenteambtenaren over privacy en gegevensuitwisseling. Destijds droeg mijn voordracht de titel 'Identiteitsfraude: U bent gewaarschuwd.' Specifiek zei ik daarover het volgende: "De Nederlandse Vereniging van Banken (NVB) heeft recent nog een campagne gehouden om burgers te waarschuwen voor de kenmerken van betrouwbare en onbetrouwbare websites voor internetbankieren. Mooie actie, zult u misschien denken. Bewustwording is een belangrijke eerste stap om identiteitsfraude tegen te gaan. De vraag is echter wat als men deze bewustwordingscampagnes gaat gebruiken als verdediging tegen slachtoffers van identiteitsfraude. Als een slachtoffer, nadat haar bankrekening leeg geroofd is door een vindingrijke fraudeur, bij de bank aanklopt zal de medewerker dan met een uiterst vriendelijke stem zeggen 'Maar mevrouw, wij hebben u toch gewaarschuwd?'

Deze 'voorspelling', hetzij op zeer beperkte schaal en met een minder cynische ondertoon, is inmiddels uitgekomen. Op zaterdag 15 september verwelkomde consumentenprogramma Kassa! enkele slachtoffers van fraude met internetbankieren. Deze slachtoffers, in tegenstelling tot de meeste anderen, waren door de Rabobank niet schadeloos gesteld. Enkele weken later, op 13 oktober, besteedde Kassa! wederom aandacht aan een slachtoffer van fraude die niet schadeloos gesteld was door een bank, ditmaal de ABN AMRO. Het tij ten aanzien van het schadeloos stellen van slachtoffers, wanneer hun bankrekening leeg geroofd is door een crimineel, lijkt te keren. En dat roept vragen op. Moeilijk te beantwoorden vragen voor de banken. Deze bijdrage beoogt daarom een overzicht te geven over de huidige ontwikkelingen op het gebied van aansprakelijkheid bij fraude met internetbankieren. Deze worden vervolgens kort in een bredere context geplaatst om na te gaan wat voor gevolgen de huidige tendens kan hebben voor internetbankieren in het algemeen en het vertrouwen daarin in het bijzonder.

"Maar mevrouw, wij hebben u toch gewaarschuwd?"

Achtergrond

Fraude met internetbankieren was in eerste instantie een probleem waar Nederlandse banken weinig tot geen last van leken te hebben. Helemaal in vergelijking met banken elders in de wereld welke uitsluitend gebruikmaakte van single factor authenticatie, veelal gebruikersnaam en wachtwoord, voor hun cliënten. De Verenigde Staten is daar het meest vooraanstaande voorbeeld van. Het Nederlandse systeem wat gebruikmaakt van de bekende twee factor authenticatie bleek robuuster, totdat de man-in-the-middle aanval arriveerde en roet in het eten gooide. Vraag naar de omvang van het probleem begon te groeien, maar bleef enige tijd onbeantwoord. Pas eind 2010 trad de NVB voor het eerst naar buiten met een kwantitatieve indicatie van het probleem (zie tabel 1).

Duidelijk wordt uit de cijfers van de afgelopen tijd dat de schade jaarlijks toeneemt. Deze stijging lijkt op het eerste oog zorgwekkend, maar relatief gezien blijft de schade uitermate beperkt. Zoals de NVB beschrijft in haar persbericht: "Per jaar vinden ongeveer 3 miljard transacties plaats via het internetbankieren, met een totale waarde van 3200 miljard euro. De schade van 27,3 miljoen betrof bijna 0,002% van de totale halfjaarlijkse transactieomzet." (NVB 2012) Reden tot paniek op basis van de cijfers blijft dus uit. En dat is terecht. De aansprakelijkheidskwestie daarentegen van individuele gevallen geeft wel reden tot zorg.

Jaar	Schade in euro's
2008	2,1 miljoen
2009	1,9 miljoen
2010	9,8 miljoen
2011	35 miljoen
2012 (eerste halfjaar)	27,3 miljoen

Tabel 1. Schadecijfers fraude internet bankieren

Aansprakelijkheid

Het beleid van banken in Nederland is vanaf het begin geweest dat zij in

de regel de klant schadeloos stellen, maar henzelf voldoende ruimte gunnen om per geval te beslissen. Doorgaans betekende dit concreet dat nagenoeg alle gevallen hun geld terugkregen. Een lange tijd bleef het aansprakelijkheidsfront daarom rustig. Dit was grotendeels totdat consumentenprogramma Kassa! in twee afleveringen aandacht wijdde aan slachtoffers die door de Rabobank en de ABN AMRO niet schadeloos gesteld zijn. Dit is een belangrijk teken dat de grens begint te verschuiven. Inmiddels wordt meer van de consument verwacht. Na jaren van voorlichtingscampagnes mag gerekend worden op een zeker bewustzijn aan de kant van de consument, volgens de banken. Deze verwachting geeft ook een andere invulling aan het begrip eigen schuld, hetgeen deel uitmaakt van de juridische aansprakelijkheid. De vraag is immers: In hoeverre is de schade te wijten aan 'eigen schuld' van het slachtoffer? Om deze vraag te beantwoorden worden twee maatstaven gebruikt, causaliteit en redelijkheid. Te beginnen met de tweede maatstaaf, "[d]e vraag die daarbij beantwoord dient te worden, is of [het slachtoffer] verwijtbaar of anders heeft gehandeld dan een zorgvuldig, redelijk handelend mens met het oog op zijn eigen belangen in de gegeven omstandigheden zou hebben gedaan…" (Timmer, 2012). Deze vraag is moeilijk te beantwoorden. Banken hebben ten alle tijde het recht behouden om consumenten die nalatig of onzorgvuldig gedrag hebben vertoond niet schadeloos te stellen. En daar zit de angel in het verhaal. De definitie van nalatig en onzorgvuldig gedrag is niet eenduidig. Gijs Boudewijn van de NVB bevestigd het gebrek aan eenduidigheid tijdens de uitzending van 15 september door te stellen dat: 'De termen onvoorzichtig en nalatig verschillen per geval, per klant en per bank.'

> Het Nederlandse systeem bleek robuuster, totdat de man-in-the-middle-aanval arriveerde

Gebrek aan eenduidigheid

Het gebrek aan eenduidigheid is bijzonder problematisch omdat consumenten op deze manier weinig houvast hebben. Het nodigt uit tot willekeur en enige vorm van transparantie is afwezig. In de uitzending van 15 september, bijvoorbeeld, kregen twee slachtoffers de gelegenheid om hun verhaal te vertellen. Het eerste slachtoffer, Helene Schrever, bankiert bij de ABN AMRO. Zij ontving een phishing email en werd vervolgens gebeld door 'Vanessa' van de ABN AMRO. Dirk Massink, gedupeerde klant van de Rabobank, ontving eveneens een email en een telefoontje van een nep bankmedewerker, Kimberly. In beide gesprekken werd naar de e-mails gerefereerd en gezegd dat de rekeningen doorgelopen moesten worden in verband met mogelijke 'fouten.' Daarvoor waren de e.dentifier of random reader codes nodig. De ABN AMRO stelde haar gedupeerde cliënt schadeloos. De Rabobank daarentegen niet. De Rabobank, zoals bleek uit de uitzending, acht het doorgeven van de random reader codes als onzorgvuldig en nalatig gedrag. Zelfs als klanten geloven dat zij met de bank in gesprek zijn. Ter verantwoording voor dit besluit refereert de Rabobank naar haar specifieke waarschuwingen om random reader codes nooit te delen. Volgens de Rabobank vertegenwoordiger heeft de bank gedurende een jaar een melding op het scherm van de internet bankierende klant geplaatst met dit bericht. In de ogen van de Rabobank is het geen gehoor geven aan deze melding dus onzorgvuldig en nalatig. Volgens Michel van Eeten, aanwezig bij de uitzending, zal de claim van de Rabobank voor de rechter geen stand houden. Op dat punt vrees ik dat hij ongelijk zou kunnen krijgen. En dat vergroot de onrust. Er is weinig jurisprudentie in Nederland en omringende landen over dergelijke zaken. In Duitsland is echter eerder dit jaar een soortgelijke zaak voor het hoogste gerechtshof verschenen. In die zaak was het slachtoffer evenmin schadeloos gesteld door zijn bank. Het slachtoffer diende daarom een aanklacht in tegen de Sparda bank (The Local, 2012). Daarin gaf de rechtbank het gelijk aan de bank. Een gevaarlijk precedent. De klant had geen recht op

> De grens van aansprakelijkheid begint te verschuiven

een vergoeding omdat hij de specifieke waarschuwingen van de bank, over het invoeren van meerdere tan-codes, onvoldoende had opgevolgd. Wederom geen vergoeding dus. Het bovenstaande introduceert een tweetal problemen. Het eerste probleem is de onduidelijkheid over de begrippen nalatig en onzorgvuldig gedrag. Zonder definitie van onzorgvuldig en nalatig blijven deze aan verandering onderhevig. Door de individuele toepassing komt het beleid van de banken over als inconsequent en weten consumenten niet waar zij aan toe zijn. Dit tast het vertrouwen aan. Het tweede probleem is het gebruik van waarschuwingen als instrument om de aansprakelijkheid op consumenten af te schuiven.

Glijdende schaal

Hoewel in de zojuist beschreven aflevering van Kassa! de ABN AMRO nog de bank was welke haar klanten wel schadeloos stelde, bleek dit enkele weken later niet meer het geval te zijn. Op zaterdag 13 oktober kwam Kassa! wederom met een aflevering waarin een slachtoffer, Michel Moret, van fraude met internetbankieren het woord kreeg. In tegenstelling tot de zaak bij de Rabobank was bij het ABN AMRO slachtoffer uitsluitend sprake van gebruik van malware. Enige vorm van social engineering was afwezig. Dit is een belangrijk gegeven omdat bij social engineering de verwijtbaarheid van het slachtoffer sneller een onderwerp van discussie zou kunnen zijn. Dit is bij malware, door de beperkte detectiemogelijkheden, moeilijker te verantwoorden. In dit geval, werd de eerste poging van criminelen om de cliënt geld afhandig te maken door de bank gedetecteerd. Deze belde de cliënt om te verifiëren dat hij inderdaad 10.000 euro naar een Poolse rekening wilde overmaken. Dit was niet het geval. De ABN AMRO gaf aan dat de computer van Moret geïnfecteerd was en hij werd aangeraden om een goede anti-virus software te installeren. Deze had Moret al. Daarnaast raadde de ABN AMRO aan om de computer op te laten schonen door een deskundig bedrijf. Volgens de uitzending heeft dit plaatsgevonden. Enkele weken later loopt, tijdens een overboeking, de computer vast. De volgende dag wordt bekend dat 9.500 euro alsnog richting Polen is gegaan. De ABN AMRO verzocht de cliënt om de factuur van het bedrijf dat zijn computer had opgeschoond, hetgeen Moret weigert te overhandigen. Vervolgens stuurt het externe bedrijf alsnog een getuigschrift van de geleverde dienst, maar dat is voor de ABN AMRO niet voldoende. De bank weigert Moret schadeloos te stellen omdat hij de instructies onvoldoende zou hebben opgevolgd en omdat de bank onvoldoende inzicht heeft in de manier waarop Moret zijn computer heeft opgeschoond. Dit roept de vraag op of Moret dan ook gezien wordt als onzorgvuldig en nalatig? Daarover geeft de ABN AMRO geen duidelijkheid tijdens de uitzending. Hetgeen in ieder geval wel geconcludeerd kan worden is dat de toepasbaarheid van eigen schuld groeiende lijkt te zijn, waarbij deze niet alleen ter sprake komt bij slachtoffers van social engineering maar ook van malware. Dat lijkt toch een glijdende schaal te illustreren, waarbij waarschuwingen en instructies als glijmiddel worden ingezet.

> De termen onvoorzichtig en nalatig verschillen per geval, per klant en per bank

> Er is weinig jurisprudentie over dergelijke zaken

Borgen van aansprakelijkheid

In ieder geval de ABN AMRO is van plan om per 1 januari 2013 enkele instructies ten aanzien van de beveiliging van de computer op te nemen. Deze houden bijvoorbeeld in dat gebruikers ten minste anti-virus software op hun computer dienen te hebben en alle updates geïnstalleerd hebben. Door deze instructies op te nemen in de algemene voorwaarden, krijgen zij een belangrijkere status. De cliënt gaat immers akkoord met de algemene

voorwaarden van de dienstverlener. Dit zou dus kunnen betekenen dat als een slachtoffer niet heeft voldaan aan deze voorwaarden dat hij of zij mogelijk niet schadeloos gesteld wordt. Dit kan leiden tot een significante toename van het aantal gevallen slachtoffers die zelf de opdraaien voor de fraude. Daarnaast is er nog een ander punt van discussie. Het niet voldoen aan de voorwaarden kan aanleiding zijn voor de bank om de cliënt niet schadeloos te stellen. Dit is mogelijk problematisch omdat hier een oorzaak gevolg verondersteld wordt wat wellicht niet van toepassing is. Anti-virus software en het regelmatig installeren van updates maakt gebruikers immers veiliger, niet veilig in absolute zin. Causaliteit is echter wel de andere maatstaaf voor de bepaling van eigen schuld in het aansprakelijkheidsrecht. Zoals Jaap Timmer beschrijft, "Er moet in ieder geval sprake zijn van een conditio sine qua-non verband tussen de schade en het nalaten bepaalde beveiligingsmiddelen in te zetten. Indien in een specifiek geval kan worden vastgesteld dat de schade niet was ingetreden wanneer van bepaalde maatregelen gebruik was gemaakt, is er in beginsel sprake van een conditio sine qua non-verband." (Timmer 2012) Er moet dus sprake zijn van directe causaliteit en dat is een lastige kwestie met betrekking tot fraude bij internetbankieren. Dan moet bijvoorbeeld vastgelegd worden of de gebruikte malware voor de aanval gedetecteerd had kunnen worden door de anti-virus software. Dit is zeker niet altijd het geval.

Eigen risico

De beslissingen van de Rabobank en de ABN AMRO zijn controversieel, maar niet geheel onverwacht. De algemene tendens is om de grens van verantwoordelijkheid en aansprakelijkheid te verschuiven aangezien internetbankieren dermate ingeburgerd is dat meer van consumenten verwacht mag worden. In februari van dit jaar kwam het idee van een eigen risico bij fraude met internetbankieren al ter sprake. De NVB opperde destijds het idee tijdens een discussiebijeenkomst waarin onder andere de ABN AMRO aangaf al eerder het idee intern besproken te hebben (Security.nl, 2012). Met het eigen risico wil de NVB consumenten vooral wijzen op hun eigen verantwoordelijkheid. Dat kwam ook naar voren tijdens de uitzending van Kassa! waarin Boudewijn benadrukte dat fraude bij internetbankieren een gezamenlijke verantwoordelijkheid kent. Dat zal niemand ontkennen, maar de verantwoordelijkheid van de consument is beperkt.

> De bank weigert schadeloosstelling omdat de instructies onvoldoende waren opgevolgd

> De beslissingen van de banken zijn controversieel

Deze beperkte verantwoordelijkheid heeft onder andere te maken met de beperkte mogelijkheden van consumenten om een aanval of een infectie te detecteren. Criminelen gaan immers steeds geavanceerder te werk waardoor hun aanvallen minder zichtbaar zijn. Zoals ik in het verleden heb beargumenteerd worden de mogelijkheden voor consumenten om zichzelf te beschermen steeds beperkter door deze dalende zichtbaarheid van aanvallen (Van der Meulen, 2011). Daarnaast heeft ook ENISA in juli nog het advies aan banken gegeven om er vanuit te gaan dat de computer van de consument geïnfecteerd is en daarop maatregelen te treffen (ENISA, 2012).

Mogelijke gevolgen

Het niet schadeloos stellen van slachtoffers, hoe beperkt ook, gaat niet geheel zonder gevolgen. Het meest in het oog springende potentieel

gevolg is een verlies van vertrouwen van consumenten in de banken en het internetbankieren. Hoewel de banken content zullen zijn met consumenten die zorgvuldiger zijn, kan dit ook doorslaan. Dat wil zeggen, consumenten kunnen in het uiterste geval internetbankieren gaan mijden en terugkeren naar ouderwets bankieren. Internet bankieren an sich wordt namelijk een risico, zelfs wanneer beveiligingsmaatregelen getroffen zijn. Een verlies van vertrouwen zou vervolgens financiële gevolgen kunnen hebben voor de banken aangezien deze ontwikkeling met grotere kosten gemoeid zou gaan.

Slachtoffers schadeloos?

Een mogelijke tweede gevolg is de roep naar betere beveiliging van internetbankieren. Dit is een ongewenste ontwikkeling. Het huidige systeem voorziet grotendeels in een balans tussen gemak en beveiliging. De hoeveelheid schade is, zoals eerder aangegeven, relatief klein waardoor een investering in meer preventiemaatregelen economisch niet per se verantwoord zou zijn. Deze gevolgen zouden meer schade en kosten kunnen opleveren dan de schade die geleden is door de slachtoffers die niet schadeloos gesteld zijn. Het is daarom ook de vraag hoeveel een dergelijke beslissing waard is voor de bank.

Als de omvang van de schade met internetbankieren relatief gezien meevalt, dan is het aantal gevallen waarvan de bank oordeelt dat het slachtoffer in kwestie onzorgvuldig heeft gehandeld nog beperkter. Daar valt financieel gezien weinig te halen. Een andere verklaring zou zijn om dit als waarschuwingssignaal richting de consument te sturen.

> Consumenten kunnen in het uiterste geval internetbankieren gaan mijden

Het altijd vergoeden van fraude met internetbankieren kan leiden tot onverschilligheid aan de kant van de consument, waardoor deze beveiliging in zijn geheel negeert. Maar dit roept wederom de vraag op hoeveel is dat signaal waard?

Conclusie

De grens van aansprakelijkheid bij fraude met internetbankieren is aan het verschuiven. De vrijblijvendheid van waarschuwingen lijkt inmiddels officieel ten einde te zijn gekomen. Deze ontwikkeling is niet geheel zonder gevolgen. De overheersende onduidelijkheid over de begrippen onzorgvuldig en nalatig is problematisch en kan leiden tot een verlies aan vertrouwen. Daarnaast is causaliteit in het geval van malware een lastige kwestie. De vraag is echter of andere banken zullen volgen. En zo ja, wanneer? Want hoewel banken het risico lopen dat consumenten digitale diensten gaan weigeren vanwege een gebrek aan vertrouwen, hangt de dreiging in de lucht. En wanneer het voorbeeld van de Rabobank en de ABN AMRO eerder regel dan uitzondering wordt zullen de zorgen voor consumenten aanzienlijk toenemen. ●

Referenties

ENISA (2012). 'Flash note: EU cyber security agency ENISA; "High Roller" online bank robberies reveal security gaps.' Beschikbaar op: http://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-201chigh-roller201d-online-bank-robberies-reveal-security-gaps (laatst geraadpleegd 31 oktober 2012).

The Local (2012). Phishing victims' losses are own fault – court. Beschikbaar op: http://www.thelocal.de/money/20120425-42161.html (laatst geraadpleegd 31 oktober 2012).

Van der Meulen, N.S. (2011). Between Awareness and Ability: Consumers and Financial Identity Theft. Communications & Strategies, First Quarter 2011: 23 – 44.

Nederlandse Vereniging van Banken (2012). 'Fraude internetbankieren stijgt eerste halfjaar met 14 %.' Beschikbaar op: http://www.nvb.nl/home-nederlands/nieuws/nieuwsberichten/fraude-internetbankieren-stijgt-eerste-half-jaar-met-14_.html (laatst geraadpleegd op 31 oktober 2012).

Security.nl (2012). 'Banken willen eigen risico voor internetbankieren.' Beschikbaar op: http://www.security.nl/artikel/40507/1/Banken_willen_eigen_risico_voor_internetbankieren.html (laatst geraadpleegd op 31 oktober 2012).

Timmer, J. (2012). Aansprakelijkheid en schadevergoeding. Beschikbaar op: http://www.iusmentis.com/aansprakelijkheid/onrechtmatigedaad/ (laatst geraadpleegd op 31 oktober 2012).